Min-entropy and quantum key distribution: non-zero key rates for "small" numbers of signals

Sylvia Bratzik,* Markus Mertz, Hermann Kampermann, and Dagmar Bruß

Institute for Theoretical Physics III, Heinrich-Heine-Universität Düsseldorf, 40225 Düsseldorf, Germany.

We calculate an achievable secret key rate for quantum key distribution with a finite number of signals, by evaluating the min-entropy explicitly. The min-entropy can be expressed in terms of the guessing probability, which we calculate for d-dimensional systems. We compare these key rates to previous approaches using the von Neumann entropy and find non-zero key rates for a smaller number of signals. Furthermore, we improve the secret key rates by modifying the parameter estimation step. Both improvements taken together lead to non-zero key rates for only $10^4 - 10^5$ signals. An interesting conclusion can also be drawn from the additivity of the min-entropy and its relation to the guessing probability: for a set of symmetric tensor product states the optimal minimum-error discrimination (MED) measurement is the optimal MED measurement on each subsystem.

I. INTRODUCTION

Quantum key distribution (QKD) is the establishment of a random secure key between two authorized parties, Alice and Bob, which are connected with each other via a quantum and a classical channel [1]. Qubits (e.g. photons) are distributed over this quantum channel, and in practical implementations the number of these particles is finite. Dealing with these finite resources, a new branch in quantum key distribution (QKD) emerged, the finite-key analysis. It investigates secure key rates, i.e. the ratio of a secure key length to the number of signals sent through the channel, in the non-asymptotic situation. The security of a finite key for a composable security definition [2–4] was proven in [5–10]. It is important to notice that composability means that the key established by QKD can be used safely in any application such as one-time-pad encryption. For a review on practical QKD and its security, see e.g. Refs. [11, 12]. Calculations of finite key rates were done in [9, 13, 14] and in [15] for d dimensions. The relevance of finite QKD was shown in [16]: practical implementations of QKD lead to a dramatically lower secure key rate in comparison to asymptotic theoretical predictions.

The paper is organized as follows: in Sec. II we describe a general QKD protocol, in Sec. III we review a bound for the statistical error in parameter estimation and show that former results on the secret key rate [9] can be improved by considering a POVM with two outcomes. In Sec. IV we concentrate on quantifying the secret key length after privacy amplification. It was found in [9, 10] that the *conditional min-entropy* gives an achievable upper bound on the secret key length. The calculation of the conditional min-entropy involves an optimization over a set of quantum states. A lower bound on the min-entropy by using the conditional von Neumann entropy was established in [9, 10]. This bound holds under the assumption of collective attacks, i.e. the state shared between Alice and Bob after Eve's interaction has tensor product structure. In Sec. V we calculate the min-entropy explicitly by applying recent results on its operational meaning [17]. For the qubit case, we evaluate the min-entropy for the BB84-protocol [1] via minimum-error discrimination (MED). For d-dimensional quantum systems, we calculate it for the generalized six-state-protocol [18, 19] via the square-root measurement. In Sec. VI we compare the key rates via calculation of the min-entropy to the bound with the von Neumann entropy. We show that our approach gives positive key rates for a smaller number of signals compared to the von Neumann approach. Furthermore we compare our results in the d-dimensional case to the recent results in [15] for the mentioned bound. We conclude in Sec. VII.

II. QUANTUM KEY DISTRIBUTION PROTOCOL

We consider an entanglement-based QKD scheme. In the following a description of the protocol will be provided.

1. *Distribution:* Alice prepares N maximally entangled states in dimension $d \times d$, where d is the dimension of the Hilbert space of a subsystem:

$$|\Phi_{00}\rangle := \frac{1}{\sqrt{d}} \sum_{x=0}^{d-1} |xx\rangle, \qquad (1)$$

and sends the second particle to Bob. In the case of qubits, i.e. $d = 2$, the state is one of the four Bell-states $|\Phi^+\rangle$. After the distribution, they share N entangled pairs, which we will denote by the state $\tilde{\rho}_{A^N B^N}$. Under the assumption of collective attacks, the state $\tilde{\rho}_{A^N B^N}$ is a tensor product state, i.e. $\tilde{\rho}_{A^N B^N} = (\rho_{AB})^{\otimes N}$ [9]. Alice and Bob can symmetrize the state ρ_{AB} by applying a depolarizing map, leading to a d^2-dimensional Bell-diagonal state [6, 7, 15]:

$$\rho_{AB} = \sum_{j,k=0}^{d-1} \lambda_{jk} |\Phi_{jk}\rangle \langle\Phi_{jk}|, \qquad (2)$$

---
* bratzik@thphy.uni-duesseldorf.de

where $|\Phi_{jk}\rangle = \frac{1}{\sqrt{d}} \sum_{s=0}^{d-1} \left(e^{\frac{2\pi i}{d}}\right)^{sk} |s\rangle |(s+j) \mod d\rangle$ are the generalized Bell states [20]. For $d = 2$, the state ρ_{AB} has the following form:

$$\rho_{AB} = \lambda_{00} P_{|\Phi^+\rangle} + \lambda_{01} P_{|\Phi^-\rangle} + \lambda_{10} P_{|\Psi^+\rangle} + \lambda_{11} P_{|\Psi^-\rangle}, \quad (3)$$

where $P_{|\psi\rangle} = |\psi\rangle\langle\psi|$, $\sum_{i,j}\lambda_{ij} = 1$ and $\{|\Phi^+\rangle, |\Phi^-\rangle, |\Psi^+\rangle, |\Psi^-\rangle\}$ is the Bell basis.

For a specific depolarizing map, one can parametrize the state ρ_{AB} by one parameter Q, which in the two-dimensional case is the *quantum bit error rate* (QBER). The relation between Q and λ_{jk} will be explained in Sec. V.

2. *Encoding and measurement:* Both parties agree on an encoding, i.e. each quantum state is associated with a symbol from an alphabet. They perform a projection measurement in certain bases.

After this step Alice and Bob will share N correlated pairs of *dits* (*d*-letter systems).

3. *Sifting:* In this step both parties announce for each qudit pair the encoding they have chosen. Depending on the protocol either they discard the data, when they differ, or they use them for parameter estimation. The bit string after this process has length $N - n'$, when n' bits were discarded.

4. *Parameter estimation* (PE): Parameter estimation serves for estimating the error in the quantum channel by using measurements, in general a positive operator valued measure (POVM). The considered state is parametrized by the quantum bit error rate (QBER) Q for $d = 2$. To measure the QBER a chosen POVM is used. Due to the finite number of signals (m randomly chosen signals are used) the QBER cannot be detected perfectly. Therefore a quantification of the statistical error is needed.

After parameter estimation the number of signal states is $n = N - n' - m$.

5. *Error correction* (EC): In this step Alice and Bob want to eliminate the error in their classical data, which might be there because of eavesdropping. In order to reconcile their data, they have to communicate publicly. In this paper, we will use known results [9] to account for the effect of error correction on the key.

6. *Privacy amplification* (PA): During the key generation, information about the key might have been revealed to the eavesdropper. To reduce this information, Alice and Bob apply a randomly chosen hash function from a family of hash functions to their identical keys.

III. IMPROVED PARAMETER ESTIMATION

Parameter estimation plays an important role in finite QKD protocols. Since one has a finite number of measurement outcomes, one needs an appropriate estimate for each parameter. In this section we first remind the reader of a method for parameter estimation used in

[9, 14, 21]. There, the parameters were estimated by different two-dimensional POVMs for different bases. We will then show that we can reach a better approximation, if we consider one specific POVM for the estimation of all parameters. The following theorem quantifies the unavoidable statistical errors in the estimated parameters.

Theorem 1. *[9, 14, 21] Let $\{B_i\}_{i=1}^{|\chi|}$ be a $|\chi|$-dimensional POVM, $\vec{\lambda}_m = (\lambda_m(1), \lambda_m(2), .., \lambda_m(|\chi|))$ and $\vec{\lambda}_\infty = (\lambda_\infty(1), \lambda_\infty(2), .., \lambda_\infty(|\chi|))$ the probability distributions, with $\lambda(i)$ being the probability of outcome B_i. Here, the index m stands for the m-fold independent application of the POVM on identical states ρ. Let now $\lambda_m := \lambda_m(k)$, $\lambda_\infty := \lambda_\infty(k)$ denote any k-th parameter. Then except with probability $\varepsilon_{\mathrm{PE}}$*

$$\frac{1}{2} ||\lambda_m - \lambda_\infty||_1 \leq \xi(\varepsilon_{\mathrm{PE}}, |\chi|, m), \quad (4)$$

$$\xi(\varepsilon_{\mathrm{PE}}, |\chi|, m) := \sqrt{\frac{\ln\left(\frac{1}{\varepsilon_{\mathrm{PE}}}\right) + |\chi| \ln(m+1)}{8m}}, \quad (5)$$

where $||A||_1 = \mathrm{tr}\sqrt{A^\dagger A}$ and $\ln$ denotes the natural logarithm [22].

Proof: See Appendix.

To clarify the influence of different choices of POVMs on secure key rates we consider a protocol, where Alice and Bob share a state, which can be parametrized by n_{PE} parameters. We choose the variables of the estimation of each parameter in a symmetric way. That means $\varepsilon_{\mathrm{PE}_i} = \frac{\varepsilon_{\mathrm{PE}}}{n_{\mathrm{PE}}}, |\chi|_i = |\chi|, m_i = \frac{m}{n_{\mathrm{PE}}}$ for all $i \in \{1, ..., n_{\mathrm{PE}}\}$, such that the constraints $\sum_{i=1}^{n_{\mathrm{PE}}} \varepsilon_{\mathrm{PE}_i} = \varepsilon_{\mathrm{PE}}$ and $\sum_{i=1}^{n_{\mathrm{PE}}} m_i = m$ are fulfilled.

In previous works [9, 14] each parameter is estimated by an individual two-dimensional POVM (in the following we will use IPOVM as an abbreviation for this approach); e.g. for the BB84 protocol, we have two parameters (error rates in two bases) to estimate. Then we need two POVMs, where each of them has two outcomes which correspond to "Alice and Bob *do have* the same measurement outcome" and "Alice and Bob *do not have* the same measurement outcome" in their respective measurement basis. This leads to $\xi(\frac{\varepsilon_{\mathrm{PE}}}{2}, 2, \frac{m}{2})$. Generally for states determined by n_{PE} we get $\xi(\frac{\varepsilon_{\mathrm{PE}}}{n_{\mathrm{PE}}}, 2, \frac{m}{n_{\mathrm{PE}}})$ for each parameter.

Concerning secure key rates we can improve this method by considering a common POVM with $n_{\mathrm{PE}} + 1$ measurement outcomes (CPOVM approach). This means for example for the BB84 protocol that we use a POVM with 3 outcomes, where two of them correspond to "Alice and Bob *do not have* the same measurement outcome" in each of the two bases and one corresponds to the completeness of the POVM. Then, the estimation of each parameter will be represented by $\xi(\varepsilon_{\mathrm{PE}}, 3, m)$. In general for $n_{\mathrm{PE}} + 1$-dimensional systems the deviation from the perfect parameter (see Eq. (4)) is given

by $\xi(\varepsilon_{\mathrm{PE}}, n_{\mathrm{PE}} + 1, m)$. The improvement is due to the fact that in Eq. (4) the trace distance is only bounded by $\xi(\varepsilon_{\mathrm{PE}}, |\chi|, m)$ and that the parameters according to the CPOVM approach lead to a smaller bound than the IPOVM approach. The results of an explicit calculation of the key rates will be provided in the last section.

IV. PRIVACY AMPLIFICATION AND THE $\bar{\varepsilon}$-SMOOTH MIN-ENTROPY

In this section, we will present some results about the min-entropy. Starting from the connection of the min-entropy to the secure key length after the *privacy amplification* step, we review the relation of the min-entropy to the guessing probability given in [17].

A. The $\bar{\varepsilon}$-smooth min-entropy and the secure key length ℓ

The $\bar{\varepsilon}$-smooth conditional min-entropy provides an upper bound for the secure key length ℓ after the *privacy amplification* step [10]:

$$\ell \lesssim H_{\min}^{\bar{\varepsilon}}(\rho_{XE}^{\otimes n} | E^n), \qquad (6)$$

where $\rho_{XE} = \sum_{x=0}^{d-1} p_x |x\rangle \langle x| \otimes \rho_E^x$ is a *classical-quantum-state*, which Alice and the eavesdropper Eve share after error correction. Here, X is Alice's random variable with values $x \in \{0, ..., d-1\}$, where d is the dimension of the quantum system. The eavesdropper holds a quantum state ρ_E^x, which is correlated with the random variable X. The symbol E^n denotes the eavesdropper's system. The parameter n is the number of signals after sifting and parameter estimation, i.e. $n = N - n' - m$.

In the following we will denote the state ρ_{XE} as a *single-signal state*, i.e. following the description above, both parties share one single state ($n = 1$). Otherwise, the state will be denoted by $\rho_{XE}^{\otimes n}$, if it has tensor product structure. We treat collective attacks, as the state shared between Alice and Eve has in this case tensor product structure. Collective attacks [23**?**] are those attacks where the eavesdropper is restricted to interact with each of the signals separately, i.e. by attaching an auxiliary system and performing unitary transformations. In [6, 7] it was shown that it suffices to consider a convex combination of product states, when analyzing the full security of QKD protocols. However, it does not follow that we can consider w.l.o.g. a product state.

We recall the definition of the $\bar{\varepsilon}$-smooth min-entropy:

Definition 1 ($\bar{\varepsilon}$-smooth min-entropy [10]). *Let $\bar{\rho}_{XE} \in \mathcal{B}^{\bar{\varepsilon}/2}(\rho_{XE}) := \{\bar{\rho}_{XE} \geq 0 : \|\bar{\rho}_{XE} - \rho_{XE}\|_1 \leq \bar{\varepsilon}\}$. The $\bar{\varepsilon}$-smooth min-entropy is defined as:*

$$H_{\min}^{\bar{\varepsilon}}(\rho_{XE} | E) := \sup_{\bar{\rho}_{XE}} H_{\min}(\bar{\rho}_{XE} | E), \qquad (7)$$

with

$$H_{\min}(\bar{\rho}_{XE} | E) = \sup_{\sigma_E} \left[-\log_2 \left(\min \lambda : \lambda \cdot \mathbb{1}_X \otimes \sigma_E \geq \bar{\rho}_{XE} \right) \right].$$
$$(8)$$

The optimization in Eq. (7) is done over the states $\bar{\rho}_{XE}$ in the $\bar{\varepsilon}$-environment of ρ_{XE}, whereas the optimization in Eq. (8) is over all states σ_E.

B. The min-entropy and the guessing probability

The evaluation in Eq. (7) is a convex optimization problem. It was shown in [17], that the min-entropy can be rewritten as the negative logarithm of the optimal guessing probability $\mathrm{p}_{\mathrm{guess}}$:

$$H_{\min}(\rho_{XE} | E) = -\log_2 \mathrm{p}_{\mathrm{guess}}, \qquad (9)$$

where

$$\mathrm{p}_{\mathrm{guess}} \equiv \mathrm{p}_{\mathrm{guess}}(X|E) := \max_{\{E_E^x\}} \sum_{x=0}^{d-1} p_x \mathrm{tr}(E_E^x \rho_E^x). \qquad (10)$$

Here it was used that the initial state ρ_{XE} is a classical-quantum state (see above), which is shared between Alice and Eve, the eavesdropper. The set $\{E_E^x\}$ denotes the POVM elements of Eve, which she uses in order to distinguish her nonorthogonal ancilla states ρ_E^x. If she could perfectly discriminate them, she would know the value of Alice's random variable X and therefore the content of the secret key.

V. EVALUATION OF THE GUESSING PROBABILITY

In this section we will present an explicit calculation of the guessing probability in Eq. (10) for d-dimensional quantum systems for the generalized six-state-protocol via *square-root measurement* (see e.g. [24–29]), and for qubit-systems ($d = 2$) for the BB84-protocol via *minimum-error discrimination* [26, 30–33]. The problem of distinguishing two mixed quantum states with minimum error was solved by Helstrøm [32], but for more states it becomes more involved. For quantum states with a certain symmetry, optimal measurements were found (see e.g. [29]), whereas for arbitrary states only bounds exist [34]. Finally, we draw a conclusion from the additivity of the min-entropy for tensor product states: for a set of symmetric tensor product states the optimal minimum-error discrimination (MED) measurement is the optimal MED measurement on the subsystems.

A. Generalized six-state-protocol for d-dimensional quantum systems

In this part we consider a $(d+1)$-bases protocol, which was introduced in [35–37]. It is a generalization of the

six-state protocol [18, 19]. We further assume a collective eavesdropping attack. Due to symmetrizations [6] the eavesdropper is forced to introduce the same error in each measurement basis. This symmetrization leads to the following Bell-diagonal state shared between Alice and Bob (see Section II):

$$\rho_{AB} = (\beta_0 - \beta_1) |\Phi_{00}\rangle \langle \Phi_{00}| + \frac{\beta_1}{d} \mathbb{1}_{d^2}, \qquad (11)$$

with $\beta_0 + (d-1)\beta_1 = 1$, $0 \leq \beta_1 < \frac{1}{d} < \beta_0 \leq 1$ and $\mathbb{1}_{d^2}$ being the identity matrix of size d^2. Note that this form is equal to the one considered in [38, 39]. The parameter β_0 can be seen as the probability that both get the same output, whereas β_1 denotes the probability that they get a particular other one. The error rate Q is given by $Q := 1 - \beta_0 = (d-1)\beta_1$; for $d = 2$, Q is the quantum bit error rate β_1. The state in Eq. (11) can be recovered from Eq. (2) by setting $\lambda_{00} = 1 - \frac{d+1}{d}(1 - \beta_0)$ and all other $\lambda_{jk} = \frac{(1-\beta_0)}{d(d-1)} = \frac{\beta_1}{d}$.

We assume that Eve holds a purification $|\psi_{ABE}\rangle$. Eve's reduced state is [38]

$$\rho_E = \frac{1}{d} \left(\beta_0 \sum_{x=0}^{d-1} |E_{xx}\rangle \langle E_{xx}| + \beta_1 \sum_{\substack{x,y \\ y \neq x}} |E_{xy}\rangle \langle E_{xy}| \right), \qquad (12)$$

and we define the normalized states ρ_E^x as:

$$\rho_E^x := \beta_0 |E_{xx}\rangle \langle E_{xx}| + \beta_1 \sum_{y \neq x} |E_{xy}\rangle \langle E_{xy}|, \qquad (13)$$

such that Eve's state is given by $\rho_E = \frac{1}{d} \sum_x \rho_E^x$. Eve's ancilla states $|E_{xy}\rangle$ have a specific form in order to fulfill the requirement in Eq. (11). They can be written in terms of an orthonormal basis of Eve $\{|f_{i,j}\rangle_E\}$:

$$|E_{xy}\rangle = \begin{cases} \frac{1}{\sqrt{\beta_0}} \sum_{k=0}^{d-1} \sqrt{\lambda_{0,k}} \omega^{xk} |f_{0,k}\rangle_E & \text{for } x = y \\ \frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} \omega^{xk} |f_{y-x,k}\rangle_E & \text{for } x \neq y, \end{cases} \qquad (14)$$

with $\omega := e^{2\pi i/d}$ and $\lambda_{j,k}$ given above. The ancilla states with $x = y$ have a fixed angle between each other, they are called pyramid states [39]. They fulfill

$$\langle E_{xy}|E_{x'y'}\rangle = \begin{cases} 1 & \text{if } x = x' \text{ and } y = y', \\ 1 - \frac{\beta_1}{\beta_0} & \text{if } x = y \neq x' = y', \\ 0 & \text{otherwise.} \end{cases}$$

The eavesdropper would like to know Alice's and Bob's classical value x and y, respectively. For the case $x \neq y$ she knows both values with certainty, as those ancilla

states are orthogonal and she can perfectly discriminate them. For the case $x = y$, Eve has to discriminate d pyramid states. Measurements for such symmetrical states exist, and it is known that the error-minimizing measurement for such states is the *square-root measurement* [24–29]. The following results for the tomographic protocol were derived in [39, 40]:

The state in Eq. (12) can be rewritten as:

$$\rho_E = \beta_0 \rho^{(=)} + (1 - \beta_0) \rho^{(\neq)}, \qquad (15)$$

where the density operator $\rho^{(=)} = \frac{1}{d} \sum_{x=0}^{d-1} |E_{xx}\rangle \langle E_{xx}|$ denotes the cases, when Alice and Bob have the same values, whereas in the case of $\rho^{(\neq)} = \frac{1}{d(d-1)} \sum_{y \neq x} |E_{xy}\rangle \langle E_{xy}|$ their values are different. The eavesdropper wants to find their common values, so she wants to discriminate those ancilla states for $x = y$. The POVM elements $|e_{xx}\rangle \langle e_{xx}|$, that discriminate the pyramid states with minimum error, are given via

$$|e_{xx}\rangle = \frac{1}{\sqrt{d\rho^{(=)}}} |E_{xx}\rangle,$$

i.e. the name *square-root measurement* is related to the construction of the elements. An explicit calculation for the operator $\frac{1}{\sqrt{d\rho^{(=)}}}$ results in [39]:

$$\frac{1}{\sqrt{d\rho^{(=)}}} = \frac{(r_0 + \sqrt{r_0 r_1} + r_1)\mathbb{1} - \rho^{(=)}}{\sqrt{r_0 r_1}(\sqrt{r_0} + \sqrt{r_1})},$$

where $r_0 = 1 - \frac{d-1}{d}\frac{\beta_1}{\beta_0}$ is the eigenvalue corresponding to the eigenvector $\sum_x |E_{xx}\rangle$ and $r_1 = \frac{\beta_1}{d\beta_0}$ is the $(d-1)$-fold eigenvalue for the eigenvector $(|E_{xx}\rangle - \frac{1}{d}\sum_y |E_{yy}\rangle)$. From this the overlap $\langle e_{xx}|E_{yy}\rangle$ can be calculated as

$$\langle e_{xx}|E_{yy}\rangle = \sqrt{\eta_0}\delta_{xy} + \sqrt{\eta_1}(1 - \delta_{xy}),$$

with $\sqrt{\eta_0} = \frac{\sqrt{r_0} + (d-1)\sqrt{r_1}}{\sqrt{d}}$, $\sqrt{\eta_1} = \frac{\sqrt{r_0} + \sqrt{r_1}}{\sqrt{d}}$ and δ_{xy} the Kronecker delta. The probability η_0 denotes the probability that Eve, when finding $|e_{xx}\rangle$, knows that Alice and Bob share the value x and η_1 denotes the probability that they hold one of the other $d - 1$ values.

The eavesdropper's probability to guess the right value of Alice consists of the following parts: the probability $(1 - \beta_0)$ that the density operator $\rho^{(\neq)}$ appears (see Eq. (15)) and the probability β_0 that $\rho^{(=)}$ appears multiplied with the probability that she guesses the right value in this case, which was η_0 (see above). Inserting r_0 and r_1 into η_0, we get an expression for the guessing probability depending on d and the error rate $Q = 1 - \beta_0$:

$$p_{\text{guess}}^{\text{six-state}}(d, Q) = 1 - \beta_0 + \beta_0 \eta_0 = Q + \frac{(1-Q)}{d}\left[1 - \frac{(d-2)Q}{d(Q-1)} + 2(d-1)\sqrt{\frac{dQ - (d+1)Q^2}{(d-1)d^2(1-Q)^2}}\right]. \qquad (16)$$

B. BB84 for qubit-systems

A strategy to distinguish two nonorthogonal quantum states is called minimal-error discrimination (MED) (see [26, 30–33]). In MED for each measurement one has a conclusive result, but with probability p_{err} the result is erroneous. It was shown by Helstrøm [32] that the maximal probability to make a correct guess when distinguishing two quantum states ρ_E^0 and ρ_E^1 that appear with the same probability $p_0 = p_1 = \frac{1}{2}$ is given by

$$p_{\text{guess}}(2, Q) = 1 - p_{\text{err}}^{\min} = \frac{1}{2}\left(1 + \frac{1}{2}\left\|\rho_E^0 - \rho_E^1\right\|_1\right). \quad (17)$$

In order to calculate $\left\|\rho_E^0 - \rho_E^1\right\|_1$, we express the states ρ_E^0 and ρ_E^1 (see Eq. (13)) in terms of the computational basis of Eve.

Assuming that Eve has a purifying system of the state in Eq. (3), and that Alice and Bob perform a von Neumann measurement, one can derive an expression for $\left\|\rho_E^0 - \rho_E^1\right\|_1$ for the BB84-protocol. The operator $\rho_E^0 - \rho_E^1$ can be written as

$$\rho_E^0 - \rho_E^1 = 2\sqrt{\lambda_{00}\lambda_{01}}\left(|00\rangle\langle01| + |01\rangle\langle00|\right)$$
$$+ 2\sqrt{\lambda_{10}\lambda_{11}}\left(|10\rangle\langle11| + |11\rangle\langle01|\right), \quad (18)$$

so

$$|\rho_E^0 - \rho_E^1| = 2\sqrt{\lambda_{00}\lambda_{01}}\left(P_{|00\rangle} + P_{|01\rangle}\right)$$
$$+ 2\sqrt{\lambda_{10}\lambda_{11}}\left(P_{|10\rangle} + P_{|11\rangle}\right), \quad (19)$$

with $|A| = \sqrt{A^\dagger A}$. The eigenvalues $2\sqrt{\lambda_{00}\lambda_{01}}$ and $2\sqrt{\lambda_{10}\lambda_{11}}$ occur with multiplicity 2. Thus the 1-norm is

$$\frac{1}{2}\left\|\rho_E^0 - \rho_E^1\right\|_1 = 2\sqrt{\lambda_{00}\lambda_{01}} + 2\sqrt{\lambda_{10}\lambda_{11}}. \quad (20)$$

The error rates in the z- and x-direction are $e_z = \lambda_{10} + \lambda_{11}$ and $e_x = \lambda_{01} + \lambda_{11}$ (see [10, 12]). There remains one free parameter, that we have to optimize to obtain the best case for Eve. We adopt the method in [12, Appendix A] to maximize the probability of correct guess in Eq. (17): according to [12], we choose $\lambda_{00} = (1-Q)(1-u)$, $\lambda_{01} = (1-Q)u$, $\lambda_{10} = Q(1-v)$ and $\lambda_{11} = Qv$, with $u, v \in [0, 1]$ and the additional constraint (from $\lambda_{01} + \lambda_{11} = Q$)

$$(1 - Q)u + Qv = Q. \quad (21)$$

Defining $|\Phi_{ij}\rangle$ as the corresponding Bell states to the value λ_{ij}, the purification of the state ρ_{AB} can be written as $|\psi_{ABE}\rangle = \sum_{ij}\sqrt{\lambda_{ij}}|\Phi_{ij}\rangle_{AB} \otimes |e_{ij}\rangle_E$, where $\{|e_{ij}\rangle\}$ is a four-dimensional orthonormal basis. Using Eq. (20) and the constraint given in Eq. (21) we find a function, which depends on the parameter v:

$$\frac{1}{2}\left\|\rho_E^0 - \rho_E^1\right\|_1 = f(v) := 2\sqrt{(1-v)\,Q\,[1 + (v-2)\,Q]}$$
$$+ 2\sqrt{(1-v)\,v\,Q^2}. \quad (22)$$

Finding the maximum of the expression leads to the result $u = v = Q$ and finally to the expressions of λ_{ij}: $\lambda_{00} = (1-Q)^2$, $\lambda_{01} = \lambda_{10} = (1-Q)Q$ and $\lambda_{11} = Q^2$. This gives the guessing probability:

$$p_{\text{guess}}^{\text{BB84}}(2, Q) = \frac{1}{2}\left(1 + 2\sqrt{(1-Q)Q}\right). \quad (23)$$

By using the same methods we can derive the guessing probability for the six-state protocol, which lead to the same result as derived in Eq. (16):

$$p_{\text{guess}}^{\text{six-state}}(2, Q) = \frac{1}{2}\left(1 + \sqrt{Q(2 - 3Q)} + Q\right). \quad (24)$$

C. Optimal multistate MED measurement from additivity of min-entropy

We know from [10] that the min-entropy is additive, i.e. for tensor product states $\rho_{XE}^{\otimes n}$ it holds that $H_{\min}(\rho_{XE}^{\otimes n}|E^n) = nH_{\min}(\rho_{XE}|E)$. The min-entropy is a function of the probability of a correct guess of Eve's states. The state $\rho_{XE}^{\otimes n}$ is of the form:

$$\rho_{XE}^{\otimes n} = \left(\frac{1}{d}\sum_{x=0}^{d-1}|x\rangle\langle x| \otimes \rho_E^x\right)^{\otimes n} \quad (25)$$

$$= \frac{1}{d^n}\sum_{\mathbf{x}\in\{0,...,d-1\}^n}|\mathbf{x}\rangle\langle\mathbf{x}| \otimes \rho_{E^n}^{\mathbf{x}}, \quad (26)$$

where

$$\rho_{E^n}^{\mathbf{x}} = \bigotimes_{i=0}^{n-1}\rho_E^{x_i} \quad (27)$$

and $\mathbf{x} = (x_0, ..., x_{n-1})$ is a vector of length n with $x_i \in \{0, ..., d-1\}$. Thus, Eve's state is given by

$$\rho_E^{\otimes n} = \frac{1}{d^n}\sum_{\mathbf{x}}\rho_{E^n}^{\mathbf{x}} \quad (28)$$

and is a sum of tensor product states, see Eq. (27). The explicit minimum-error discrimination problem is to distinguish the set of states $\{\rho_{E^n}^{\mathbf{x}}\}$ for different $\mathbf{x}$. We can conclude from the additivity of the min-entropy, that for the set of states given in Eq. (27) the optimal MED measurement consists of optimal MED measurements on the single-signal states $\rho_E^{x_i}$. This result is interesting, as in general measurements in the total Hilbert space may lead to higher guessing probabilities than measurements in individual subspaces. To the best of our knowledge, this result is not known in the context of state discrimination.

VI. COMPARISON OF KEY RATES

In this chapter we provide the results of parameter estimation with CPOVM (see Sec. III) and those of the

calculation of the min-entropy (see Sec. V). We first review some results about finite-key distribution.

For a finite number of signals, the achievable secure key rate is found to be [9, 14]:

$$\ell_1/N = \frac{n}{N}\left(S_\xi(\rho_{XE}|E) + \Delta - \text{leak}_{\text{EC}}\right) + \frac{2}{N}\log_2\left(2\varepsilon_{\text{PA}}\right),$$
(29)

with $\Delta := -7\sqrt{\frac{\log_2(2/\bar{\varepsilon})}{n}}$, the total security parameter ε (see e.g. [14, 21])

$$\varepsilon = \varepsilon_{\text{PA}} + \varepsilon_{\text{EC}} + \varepsilon_{\text{PE}} + \bar{\varepsilon}$$
(30)

and $S_\xi(\rho_{XE}|E) := \min_{\bar{\rho}_{XE}\in\Gamma_\xi} S(\rho_{XE}|E)$. The set $\Gamma_\xi = \{\sigma : \frac{1}{2}|\lambda_m - \lambda_\infty(\sigma)| \leq \xi\}$ contains all states compatible with the statistics in parameter estimation. The conditional von Neumann entropy with the correction term Δ is a lower bound on the $\bar{\varepsilon}$-smooth min-entropy. The leakage term leak_{EC} is taken from [12] to be $\text{leak}_{\text{EC}} = 1.2h(Q)$ for $\varepsilon_{\text{EC}} = 10^{-10}$, where $h(x)$ is the binary entropy. Throughout all calculations, we assume asymmetric protocols with a symmetric attack. An asymmetric protocol means that one only keeps the measurement results of one particular basis for the key; the other results are used for parameter estimation. In the case of protocols with $(d+1)$ bases (e.g. the six-state protocol with $d = 2$) this basis is chosen with probability $q = (1 - dp)$ and the other d bases with probability p. For protocols with 2 bases (e.g. the BB84-protocol with $d = 2$) $q = 1 - p$. Taking the largest deviation ξ_i from the perfect parameter in one measurement basis and equating it with the other deviations, leads to a symmetric choice of parameters m_i and $\varepsilon_{\text{PE}_i}$, i.e. $m_i = \frac{m}{d+1}$ ($m_i = \frac{m}{2}$ for $2-$bases protocols) and $\varepsilon_{\text{PE}_i} = \frac{\varepsilon_{\text{PE}}}{d+1}$ ($\varepsilon_{\text{PE}_i} = \frac{\varepsilon_{\text{PE}}}{2}$) (see section III). This assumption gives a lower bound on the secret key rate. The number of signals used for parameter estimation is given by $m = Np^2$.

In order to calculate the key rate, we fix ε and ε_{EC} and maximize ℓ_1/N in Eq. (29) for the parameters $\varepsilon_{\text{PE}}, \varepsilon_{\text{PA}}, \bar{\varepsilon}$ and q with a computational software program (Mathematica) under the constraint given in Eq. (30).

A. Key rates via von Neumann entropy for different approaches of parameter estimation

For a comparison of the approaches (IPOVM, CPOVM) explained in Sec. III we consider the asymmetric BB84- and six-state-protocol for a symmetric attack for dimension $d = 2$ as discussed in [9]. In the calculation of the key rates via the von Neumann entropy (see Eq. (29)) we use a QBER of $Q = 0.05$ and a total security parameter of $\varepsilon = 10^{-9}$ (see Eq. (30)). The conditional von Neumann entropy for the six-state protocol is given by [9, 12]:

$$S^{\text{six-state}}(\rho_{XE}|E) = (1 - Q)\left[1 - h\left(\frac{1 - \frac{3}{2}Q}{1 - Q}\right)\right]$$
(31)

and for the BB84-protocol

$$S^{\text{BB84}}(\rho_{XE}|E) = 1 - h(Q).$$
(32)

The variables ξ for parameter estimation used in this comparison are summarized in Tab. I. Note that the symmetrized state is parametrized by only one parameter. This has no influence on the IPOVM approach, in contrast to CPOVM, where the number of POVM outcomes can be reduced from 3 for BB84 (4 for six-state) to 2 (2).

	BB84	six-state
IPOVM	$\xi(\frac{\varepsilon_{\text{PE}}}{2}, 2, \frac{m}{2})$	$\xi(\frac{\varepsilon_{\text{PE}}}{3}, 2, \frac{m}{3})$
CPOVM	$\xi(\varepsilon_{\text{PE}}, 2, m)$	$\xi(\varepsilon_{\text{PE}}, 2, m)$

TABLE I. Deviations ξ from perfect parameter (see Eq. (4) in Sec. III) for different parameter estimation approaches (IPOVM and CPOVM): BB84 and six-state protocol.

The results are shown in Fig. 1 and 2. We point out that our CPOVM approach leads to higher key rates for the BB84- and six-state-protocol. In particular for signals $N \lesssim 10^{11}$, the numerical analysis reveals the importance of parameter estimation. While the CPOVM approach leads for $N = 10^6$ signals to a 72% (35%) higher key rate than the IPOVM approach for the six-state- (BB84-) protocol, the improvement for $N = 10^{10}$ is still 3% (2%).
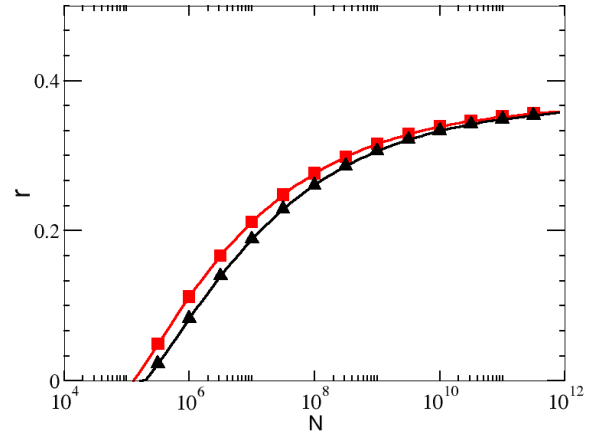

FIG. 1. (Color online) Comparison of the key rates (calculated via the von Neumann entropy, see Eqs. (29) and (32)) using different parameter estimations for asymmetric BB84-protocol; $\varepsilon = 10^{-9}$, $Q = 5\%$; squares (red): CPOVM, triangles (black): IPOVM (see Sec. III for explanations).

B. Key rates via the min-entropy for two-dimensional quantum systems

In this section we exploit the preceding results from Sec. V regarding the min-entropy in order to compute the
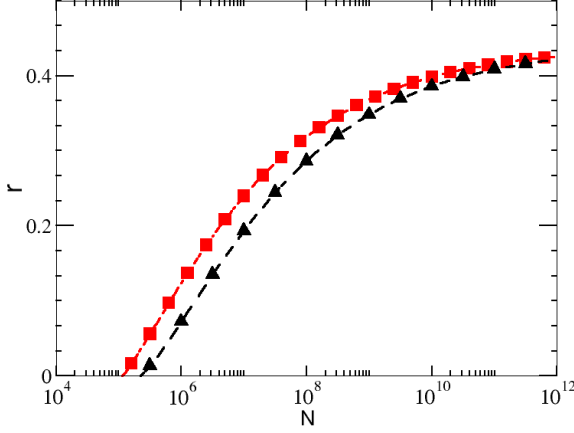
FIG. 2. (Color online) Comparison of the key rates (calculated via the von Neumann entropy, see Eqs. (29) and (31)) using different parameter estimations for asymmetric six-state-protocol; $\varepsilon = 10^{-9}, Q = 5\%$; squares (red): CPOVM, triangles (black): IPOVM (see Sec. III for explanations).

FIG. 3. (Color online) Threshold value N_0 (number of signals, where the key rate becomes non-zero) vs QBER Q with $\varepsilon = 10^{-9}$ and $\varepsilon_{\mathrm{EC}} = 10^{-10}$; triangles (red): BB84-protocol, squares (black): six-state-protocol; filled: min-entropy (Eq. (34)), open: von Neumann entropy with CPOVM approach (Eq. (29)), dashed line: von Neumann entropy (Eq. (29)) with IPOVM approach (see Sec. III for explanations).

secret key rate and compare it to the key rate calculated with Eq. (29).

We explained in Sec. IV that the achievable upper bound on the secure key length ℓ after the *privacy amplification* step is given by Eq. (6). We can derive a key rate by using the following bounds [10, Lemma 3.2.6]:

$$H_{\min}^{\bar{\varepsilon}}(\rho_{XE}^{\otimes n}|E^n) \geq nH_{\min}^{\bar{\varepsilon}/n}(\rho_{XE}|E) \geq nH_{\min}(\rho_{XE}|E);$$
$$(33)$$

the last inequality is a very good approximation as $\bar{\varepsilon}$ is in the order of 10^{-10}. Thus, we arrive at the following key rate:

$$\ell_2/N = \frac{n}{N}\left(H_{\min,\xi}(\rho_{XE}|E) - \mathrm{leak}_{\mathrm{EC}}\right) + \frac{2}{N}\log_2\left(2\varepsilon_{\mathrm{PA}}\right),$$
$$(34)$$

where the leakage term $\mathrm{leak}_{\mathrm{EC}}$ and $\varepsilon_{\mathrm{PA}}$ are the same as in Eq. (29), and $H_{\min,\xi}(\rho_{XE}|E) := \min_{\bar{\rho}_{XE} \in \Gamma_\xi} H_{\min}(\rho_{XE}|E)$ (see Eq. (29)). We calculate this key rate using the connection to the guessing probability, i.e. $H_{\min}^{\mathrm{protocol}}(\rho_{XE}|E) = -\log_2 p_{\mathrm{guess}}^{\mathrm{protocol}}$ (see Eq. (9)), and compare it to the key rate given in Eq. (29). The guessing probability for the specific protocol is given by Eqs. (23) and (24).

In Fig. 3 the threshold number of signals N_0, where the key rate becomes non-zero, is plotted as a function of the QBER Q. For parameter estimation, we have considered the CPOVM approach (see Sec. III) with the variables given in Tab. I. Additionally, we have plotted the key rate via the von Neumann entropy (Eq. (29)) for the IPOVM approach. In comparison to the von Neumann approximation (Eq. (29)), only 1/2 (7/10) of the number of signals is needed for non-zero key rates in the six-state-protocol for $Q = 0.2\%$ ($Q = 3.8\%$), when using the min-entropy. For the BB84-protocol, only 1/2 (9/10) of the number of signals is needed for $Q = 0.2\%$ ($Q = 3.8\%$).
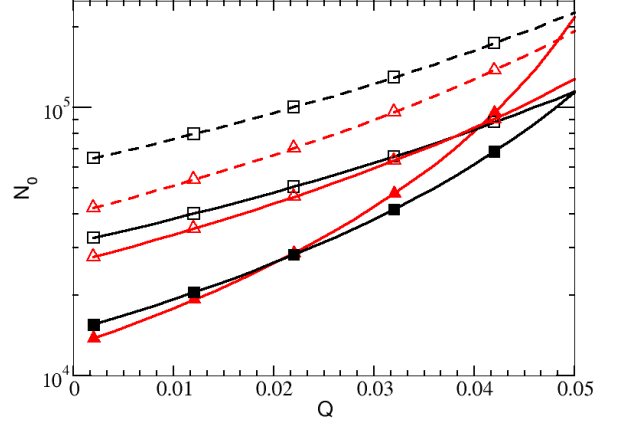
Thus, by calculating a key rate explicitly with the min-entropy, we get positive key rates for a smaller number of signals than via the von Neumann entropy approach. This behavior can be explained by the correction term Δ in the key rate in Eq. (29). For a small number of total signals N, this correction term is not a good approximation and has a big impact on the key rate.

We point out that for low Q we can achieve non-zero key rates with only $\mathcal{O}(10^4) - \mathcal{O}(10^5)$ signals. Note that in [41] it was considered a "milestone" to reach non-zero key rates for significantly less than $10^5 - 10^6$ signals.

C. Key rates via the min-entropy for d-dimensional quantum systems

In [15] the influence of the dimension on the key rate was discussed. Exploiting the results from this paper, we discuss the improvement for higher-dimensional quantum systems. Throughout this part we only consider the $(d+1)$-bases protocols, such as the six-state-protocol for $d = 2$. Furthermore, we adapt our CPOVM approach and by using Eq. (4) from Sec. III we get $\xi(\varepsilon_{\mathrm{PE}}, 2, m)$. The correction term to the d-dimensional von Neumann entropy is given in [42] as $\Delta = -(2\log_2 d + 3)\sqrt{\frac{\log_2(2/\bar{\varepsilon})}{n}}$ and the leakage term is characterized by $\mathrm{leak}_{\mathrm{EC}} = 1.2 h_d(Q)$ with $h_d(p) := -p\log_2\left(\frac{p}{d-1}\right) - (1-p)\log_2(1-p)$. The conditional von Neumann entropy was calculated in

[15] as

$$S^d(\rho_{XE}|E) = (1 - Q)\left[\log_2 d - h_d\left(1 - \frac{1 - \frac{d+1}{d}Q}{1 - Q}\right)\right],$$
(35)

where $Q = 1 - \beta_0$ denotes the error rate in the sifted key. We will compare the key rate calculated via the d-dimensional conditional von Neumann entropy, with the one via the d-dimensional min-entropy. The latter can be obtained by using

$$H_{\min}^d(\rho_{XE}|E) = -\log_2 p_{\text{guess}}(d, Q),$$
(36)

where $p_{\text{guess}}(d, Q)$ was given in Eq. (16).

In order to quantify the number of signals, we have scaled N_0 with $\log_2 d$, as for example sending one state in the dimension $d = 4$ corresponds to sending two states in the dimension $d = 2$. For making the key rate comparable to the two-dimensional case, it has to be divided by $\log_2 d$. The dimensions are prime numbers as complete mutually unbiased bases can be formed for primes and prime powers (see e.g. review article [43]).
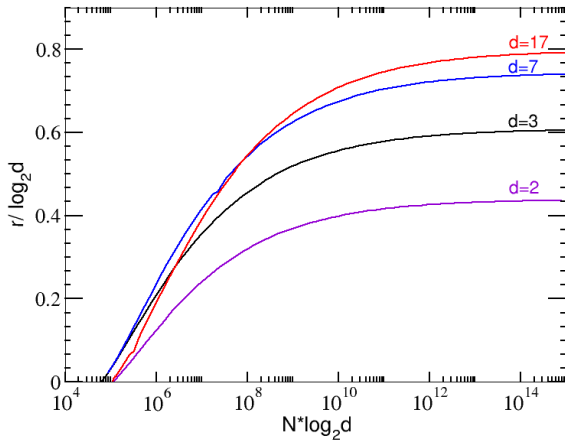

FIG. 4. (Color online) Key rates with d-dimensional conditional von Neumann entropy (Eq. (35)) plotted versus scaled total number of signals for a fixed error rate $Q = 5\%$. This is analogous to [15], where a different scale was used for the axes.

Figure 4 shows the behavior of the key rate calculated with Eq. (35) for different dimensions. In contrast to [15], we scaled the key rate with the dimension. It can be seen from the plot, that higher dimensions are advantageous as the key rate increases. In order to obtain the behavior for a small number of signals, Fig. 5 provides a magnification of this area. The higher the dimension, the more the point, where the key rate becomes non-zero is shifted to the right (apart from the case $d = 2$). This might be due to the correction term, as it scales linearly with the dimension, so for higher dimension, more is subtracted from the conditional von Neumann entropy. We will see in the next paragraph, that the min-entropy ap-
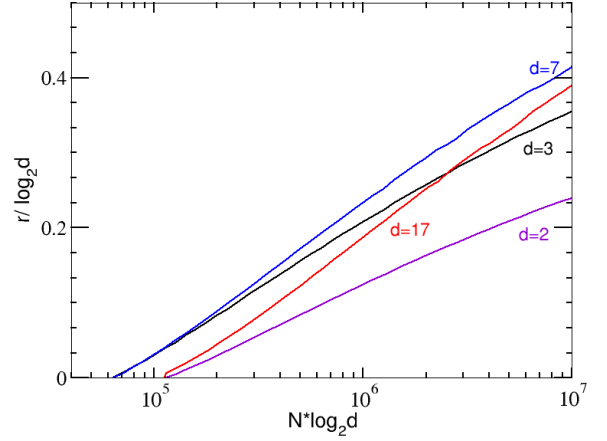

FIG. 5. (Color online) Key rates with d-dimensional conditional von Neumann entropy (Eq. (35)) plotted versus scaled total number of signals for a fixed error rate $Q = 5\%$ (Magnification of Fig. 4).

proach has an advantage over the von Neumann entropy approach for a small number of signals.
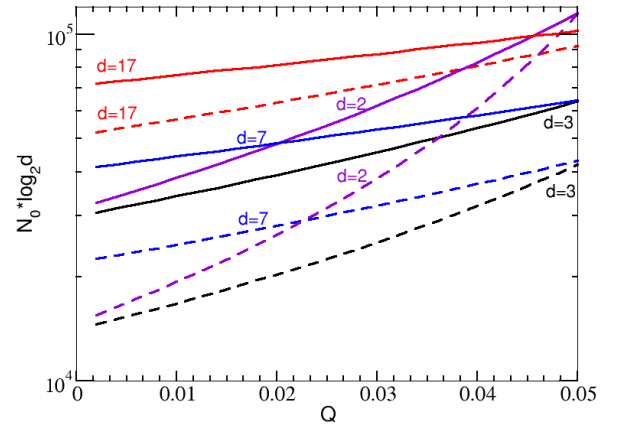

FIG. 6. (Color online) Threshold value N_0 (number of signals, where the key rate is positive) vs QBER with $\varepsilon = 10^{-9}$ and $\varepsilon_{\text{EC}} = 10^{-10}$ for different dimensions $d \in \{2, 3, 7, 17\}$. Dashed line: min-entropy (Eq. (36)), straight line: von Neumann entropy (Eq. (35)).

In Fig. 6 we compare the number N_0, where the key rate becomes non-zero, for key rates using the quantities given in Eqs. (35) and (36) for different dimensions. It can be seen that the min-entropy approach is better throughout the presented error rates. The advantage of the min-entropy approach (Eq. (36)) over the von Neumann approach (Eq. (35)) augments with increasing dimensions. This can be explained again with the correction term that scales linearly with the dimension. When comparing higher dimensions to the qubit case, one can see that for certain error rates the dimensions bigger than

two are advantegous. The dimension $d = 3$ for example, gives a lower threshold value N_0 for non-zero key rates than the qubit case throughout all the presented error rates.

VII. CONCLUSION

We have improved the secret key rates in QKD with a finite number of signals, by considering parameter estimation to be implemented by a single POVM for all parameters. Additionally, we have calculated the min-entropy for a single-signal state in d-dimensions explicitly by using its operational meaning via the guessing probability. We showed that using this ansatz for a small number of signals leads to computable non-zero key rates. This advantage of the min-entropy might be due to the correction term Δ in key rate calculations using the conditional von Neumann entropy [9, 14, 15], as this correction is big for a small number of signals. This correction term scales linearly with the dimension, so an improvement for high dimensions (up to $d = 17$) is found by calculating the min-entropy. Thus higher-dimensional systems might be advantageous when resources are limited. As a spin-off, we have deduced from the additivity property of the min-entropy and its relation to the guessing probability, that the optimal minimum-error discrimination measurement (MED) for a set of tensor product states with a certain symmetry is the optimal MED measurement on each subsystem.

Considering the importance of finite-key analysis for practical implementations, we have shown that non-zero secure key rates can be achieved already with $10^4 - 10^5$ signals per run.

Appendix A: Proof of Theorem 1

Proof. We first show that $\text{Prob} \left[\frac{1}{2} \left|\left| \vec{\lambda}_m - \vec{\lambda}_\infty \right|\right|_1 > 2\xi \right] \leq \varepsilon_{\text{PE}}$. Starting from the law of large numbers [44],

$$\text{Prob} \left[D(\vec{\lambda}_m || \vec{\lambda}_\infty) > 2\xi' \right] \leq 2^{-m\left(2\xi' - |\chi| \frac{\log_2 (m+1)}{m} \right)}, \tag{A1}$$

with $D(\vec{\lambda}_m || \vec{\lambda}_\infty) := \sum_{i=1}^{|\chi|} \lambda_m(i) \log_2 \left(\frac{\lambda_m(i)}{\lambda_\infty(i)} \right)$ and using [44]

$$\frac{1}{2} \left|\left| \vec{\lambda}_m - \vec{\lambda}_\infty \right|\right|_1 \leq \sqrt{\frac{D(\vec{\lambda}_m || \vec{\lambda}_\infty) \ln 2}{2}}, \tag{A2}$$

we result in

$$\text{Prob} \left[\frac{1}{2} \left|\left| \vec{\lambda}_m - \vec{\lambda}_\infty \right|\right|_1 > \sqrt{\frac{2\xi' \ln 2}{2}} \right]$$

$$\overset{(A2)}{\leq} \text{Prob} \left[\sqrt{\frac{D(\vec{\lambda}_m || \vec{\lambda}_\infty) \ln 2}{2}} > \sqrt{\frac{2\xi' \ln 2}{2}} \right]$$

$$\overset{(A1)}{\leq} 2^{-m\left(2\xi' - |\chi| \frac{\log (m+1)}{m} \right)}. \tag{A3}$$

For $\xi := \sqrt{\frac{2\xi' \ln 2}{2}}$ it follows:

$$\text{Prob} \left[\frac{1}{2} \left|\left| \vec{\lambda}_m - \vec{\lambda}_\infty \right|\right|_1 > 2\xi \right]$$

$$= \text{Prob} \left[\frac{1}{2} \left|\left| \vec{\lambda}_m - \vec{\lambda}_\infty \right|\right|_1 > \sqrt{\frac{2(4\xi') \ln 2}{2}} \right]$$

$$\overset{(A3)}{\leq} 2^{-m\left(2(4\xi') - |\chi| \frac{\log (m+1)}{m} \right)}$$

$$= 2^{-m\left(8 \frac{\xi^2}{\ln 2} - |\chi| \frac{\log (m+1)}{m} \right)} =: \varepsilon_{\text{PE}}.$$

Then except with probability ε_{PE}, the following holds:

$$\frac{1}{2} \left|\left| \vec{\lambda}_m - \vec{\lambda}_\infty \right|\right|_1 \leq 2\xi$$

with $\xi = \sqrt{\frac{\ln \left(\frac{1}{\varepsilon_{\text{PE}}} \right) + |\chi| \ln (m+1)}{8m}}$. It remains to show that

$$\frac{1}{2} ||\lambda_m - \lambda_\infty||_1 \equiv \frac{1}{2} |\lambda_m - \lambda_\infty| \leq \frac{1}{2} \frac{1}{2} \left|\left| \vec{\lambda}_m - \vec{\lambda}_\infty \right|\right|_1.$$

Remember that we denote by $\lambda_m := \lambda_m(k)$ and $\lambda_\infty := \lambda_\infty(k)$ any k-th parameter. The normalization conditions of the POVM $\sum_{i=1}^{|\chi|} \lambda_\infty(i) = 1 = \sum_{i=1}^{|\chi|} \lambda_m(i)$ lead to

$$|\lambda_m - \lambda_\infty| = \left| \sum_{i=1, i \neq k}^{|\chi|} \lambda_m(i) - \lambda_\infty(i) \right|$$

$$\overset{\Delta}{\leq} \sum_{i=1, i \neq k}^{|\chi|} |\lambda_m(i) - \lambda_\infty(i)| \tag{A4}$$

and

$$\sum_{i=1}^{|\chi|} |\lambda_m(i) - \lambda_\infty(i)| \overset{(A4)}{\geq} 2|\lambda_m - \lambda_\infty|.$$

The assertion follows by multiplication with factor $\frac{1}{4}$. $\quad \square$

[1] C. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India* (IEEE, New York, 1984) p. 175.

[2] M. Ben-Or and D. Mayers, "General security definition and composability for quantum classical protocols," arXiv:quant-ph/0409062.

[3] D. Unruh, "Simutable security for quantum protocols," arXiv:quant-ph/0409125.

[4] J. Müller-Quade and R. Renner, New J. Phys. **11**, 085006 (2009).

[5] R. Renner and R. König, in *Theory of Cryptography*, Lecture Notes in Computer Science, Vol. 3378, edited by J. Kilian (Springer Berlin / Heidelberg, 2005) pp. 407–425, arXiv:quant-ph/0403133.

[6] R. Renner, N. Gisin, and B. Kraus, Phys. Rev. A **72**, 012332 (2005).

[7] B. Kraus, N. Gisin, and R. Renner, Phys. Rev. Lett. **95**, 080501 (2005).

[8] M. Hayashi, Phys. Rev. A **76**, 012329 (2007).

[9] V. Scarani and R. Renner, Phys. Rev. Lett. **100**, 200501 (2008).

[10] R. Renner, Int. J. Quant. Inf. **6**, 1 (2008).

[11] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).

[12] V. Scarani, H. Bechmann-Pasquinucci, N. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, Rev. Mod. Phys. **81**, 1301 (2009).

[13] T. Meyer, H. Kampermann, M. Kleinmann, and D. Bruß, Phys. Rev. A **74**, 042340 (2006).

[14] R. Cai and V. Scarani, New Journal of Physics **11**, 045024 (2009).

[15] L. Sheridan and V. Scarani, Phys. Rev. A **82**, 030301 (2010).

[16] J. Hasegawa, M. Hayashi, T. Hiroshima, A. Tanaka, and A. Tomita, "Experimental decoy state quantum key distribution with unconditional security incorporating finite statistics," arXiv:0705.3081 [quant-ph].

[17] R. König, R. Renner, and C. Schaffner, IEEE Trans. Inf. Th. **55**, 4337 (2009), arXiv:0807.1338 [quant-ph].

[18] D. Bruß, Phys. Rev. Lett. **81**, 3018 (1998).

[19] H. Bechmann-Pasquinucci and N. Gisin, Phys. Rev. A **59**, 4238 (1999).

[20] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, Phys. Rev. Lett. **70**, 1895 (1993).

[21] V. Scarani and R. Renner, in *Theory of Quantum Computation, Communication, and Cryptography*, Lecture Notes in Computer Science, Vol. 5106, edited by Y. Kawano and M. Mosca (Springer Berlin / Heidelberg, 2008) pp. 83–95.

[22] The formula in [9, 14, 21] was corrected in an erratum [45]. The formula in Eq. (5) can be obtained by multiplying the corresponding formula in [45] by $\frac{1}{2}$.

[23] E. Biham and T. Mor, Phys. Rev. Lett. **78**, 2256 (1997).

[24] A. Holevo, Theor. Probab. Appl. **23**, 411 (1978).

[25] P. Hausladen and W. Wootters, J. Mod. Opt. **41**, 2385 (1994).

[26] M. Ban, K. Kurukowa, R. Momose, and O. Hirota, Int. J. Theor. Phys. **36**, 1269 (1997).

[27] Y. Eldar and G. Forney, IEEE Trans. Inf. Theory **47**, 858 (2001).

[28] A. Chefles, Contemp. Phys. **41**, 401 (2000).

[29] S. Barnett, Phys. Rev. A **64**, 030303 (2001).

[30] A. S. Holevo, Journal of Multivariate Analysis **3**, 337 (1973).

[31] H. Yuen, R. Kennedy, and M. Lax, IEEE Trans. on Inform. Theor. **21**, 125 (1975).

[32] C. Helstrøm, *Quantum Detection and Estimation Theory* (Academic, New York, 1976).

[33] U. Herzog and J. Bergou, Phys. Rev. A **70**, 022302 (2004).

[34] D. Qiu and L. Li, Phys. Rev. A **81**, 042329 (2010).

[35] H. Bechmann-Pasquinucci and A. Peres, Phys. Rev. Lett. **85**, 3313 (2000).

[36] D. Bruß and C. Macchiavello, Phys. Rev. Lett. **88**, 127901 (2002).

[37] N. Cerf, M. Bourennane, A. Karlsson, and N. Gisin, Phys. Rev. Lett. **88**, 127902 (2002).

[38] D. Bruß *et al.*, Phys. Rev. Lett. **91**, 097901 (2003).

[39] Y. Liang *et al.*, Phys. Rev. A **68**, 022324 (2003).

[40] D. Kaszlikowski *et al.*, Phys. Rev. A **70**, 032306 (2004).

[41] V. Scarani, in *Quantum Cryptography and Computing*, NATO Science for Peace and Security Series - D: Information and Communication Security, Vol. 26, edited by R. Horodecki, S. Y. Kilin, and J. Kowalik (2010) pp. 76–82, arXiv:1010.0521 [quant-ph].

[42] L. Sheridan and V. Scarani, Phys. Rev. A **83**, 039901 (2011).

[43] T. Durt, B.-G. Englert, I. Bengtsson, and K. Życzkowski, "On mutually unbiased bases," arXiv:1004.3348 [quant-ph].

[44] T. Cover and J. Thomas, *Elements of Information Theory* (Wiley, New York, 1991).

[45] R. Y. Q. Cai and V. Scarani, New Journal of Physics **11**, 109801 (2009).